CLAIMS:

1. A method for allowing a sender to send an encrypted message to at least one recipient from any data terminal connected to a data communications network and being capable of securely sending data to at least one computer connected to the data communications network, said method comprising:

(a) providing a virtual network connectable to the data communications network and providing access to a respective user space dedicated to the sender and each recipient for storing a respective public and a respective private key thereof, and

(b) controlling access to each user space so as to allow the sender and each recipient unrestricted access to his own user space while allowing either restricted or no access to any other user space.

2. A virtual network connectable to a data communications network for allowing a sender to send an encrypted message to at least one recipient from any data terminal connected to the data communications network, said virtual network comprising:

a respective user space dedicated to the sender and each recipient for storing a respective public and a respective private key thereof, and

at least one computer coupled to each user space for controlling access thereto so as to allow the sender and each recipient unrestricted access to his own user space for accessing his own public and private keys while allowing access to the public key only in any other user space.

3. The virtual network according to Claim 2, wherein the at least one computer serves more than one user space.

4. The virtual network according to Claim 2, wherein the at least one computer is a separate computer for each user space.

5. The virtual network according to Claim 2, wherein the respective public key of the sender and of each recipient is embedded within a certificate.

6. A method for sending an encrypted message by a sender to at least one recipient having a respective user space in the virtual network according to Claim 2, the method comprising the following steps carried out by the at least one computer coupled to the sender's user space:

(a) obtaining the respective public key of each recipient from the respective user space of each recipient,

(b) securely receiving the message from the data terminal, and

(c) encrypting the message using the respective public key of each recipient.

7. The method according to Claim 6, further including:

(d) conveying the encrypted message to the respective user space of each recipient so as to allow each recipient to access the message from any data terminal capable of securely receiving data from the at least one computer and being connected to the data communications network.

8. The method according to Claim 6, further including:

(d) signing the message with the sender's private key.

9. The method according to Claim 8, further including:

(e) conveying the encrypted message to the respective user space of each recipient so as to allow each recipient to access the message from any data terminal capable of securely receiving data from the at least one computer and being connected to the data communications network.

10. A data communications network comprising:

a virtual network allowing a sender to send an encrypted message to at least one recipient from any data terminal connected to the data communications network, said virtual network comprising:

a respective user space dedicated to the sender and each recipient for storing a respective public and a respective private key thereof, and

at least one computer coupled to each user space for controlling access thereto so as to allow the sender and each recipient unrestricted access to his own user space for accessing his own public and private keys while allowing access to the public key only in any other user space; and

a database connected to the data communications network for storing respective public keys of at least a subset of users not having respective user spaces in the virtual network.

11. A method for sending an encrypted message by a sender having a user space in the virtual network to at least one recipient via the data communications network according to Claim 10, the method comprising the following steps carried out by the at least one computer coupled to the sender's user space:

(a) obtaining the respective public key of each recipient,

(b) securely receiving the message from the data terminal, and

(c) encrypting the message using the respective public key of each recipient.

12. The method according to Claim 11, wherein step **(a)** includes:

i) obtaining the respective public key of each recipient having a user space in the virtual network from the respective user space of each recipient, and

ii) in respect of each recipient not having a user space in the virtual network, obtaining the respective public key of the recipient from the database.

13. The method according to Claim 11, further including:

(d) conveying the encrypted message to the respective user space of each recipient so as to allow each recipient to access the message from any data terminal capable of securely receiving data from the at least one computer and being connected to the data communications network.

14. The method according to Claim 11, further including:

(e) signing the message with the sender's private key.

15. The method according to Claim 14, further including:

(f) conveying the encrypted message to the respective user space of each recipient so as to allow each recipient to access the message from any data terminal capable of receiving secure data from the at least one computer and being connected to the data communications network.

16. A method for sending an encrypted message by a sender not having a user space in the virtual network to at least one recipient having a user space in the virtual network via the data communications network according to Claim 10, the method comprising the following steps carried out by the at least one computer coupled to the at least one recipient's user space:

(a) obtaining the respective public key of each recipient from the respective user space of each recipient,

(b) encrypting the message using the respective public key of each recipient, and

(c) conveying the encrypted message to the respective user space of each recipient so as to allow each recipient to access the message from any data terminal capable of securely receiving data from the at least one computer and being connected to the data communications network.

17. The method according to Claim 16, further including:

(d) signing the message with the sender's private key.

18. A program storage device readable by a computer coupled to a respective user space dedicated to a sender and at least one recipient and storing a respective public and a respective private key thereof, said program storage device tangibly embodying a program of instructions executable by the computer to perform method steps for sending an encrypted message by the sender to the at least one recipient, the method comprising the following steps:

(a) obtaining the respective public key of each recipient from the respective user space of each recipient,

(b) receiving the message from a data terminal connected to the machine via a secure communication channel,

(c) encrypting the message using the respective public key of each recipient, and

(d) conveying the encrypted message to the respective user space of each recipient so as to allow each recipient to access the message from any

data terminal capable of receiving secure data and being connected to the computer via a data communications network.

19. A computer program product comprising a computer useable medium having computer readable program code embodied therein and being executable by a computer coupled to a respective user space dedicated to a sender and at least one recipient and storing a respective public and a respective private key thereof, the computer program product comprising:

computer readable program code for causing the computer to obtain the respective public key of each recipient from the respective user space of each recipient,

computer readable program code for causing the computer to receive the message from the data terminal via a secure communication channel,

computer readable program code for causing the computer to encrypt the message using the respective public key of each recipient, and

computer readable program code for causing the computer to convey the encrypted message to the respective user space of each recipient so as to allow each recipient to access the message from any data terminal capable of receiving secure data and being connected to the computer via a data communications network.